CYBERWORX™

AIR FORCE CYBERWORX REPORT: REMODELING AIR FORCE CYBER COMMAND & CONTROL

MICHAEL V. CHIARAMONTE, Lt Col, USAF
Senior Designer & Facilitator

JEFFREY A. COLLINS, Col, USAF
Director, AF CyberWorx

COURSE DESIGN PROJECT CONDUCTED
5 Jan – 5 May 17

Produced by cadets after research with members from USAFA, USCYBERCOM, SAF/CIO A6, AFSPC, AETC, ACC, AMC, 24 AF, 25 AF, and partners in Industry & Academia

Air Force CyberWorx™
2354 Fairchild Dr, Ste 2N300
USAF Academy, CO 80840
AFCyberWorx@usafa.edu - @AFCyberWorx - (719) 333–4278

Introduction

CyberWorx is a dynamic organization partnering Airmen, industry, and academia to reimagine how technology might enrich and protect our nation, businesses, and lives. As a human-centric design center, we seek out unique ways to connect Air Force warfighters with current and future technology in meaningful ways. We look to transfer, license, and share promising prototypes, solutions, and knowledge with our partners to create value for both the warfighter and the economy as this is the best way toward operational advantage.

Design Thinking @AFCyberWorx

Design thinking is an innovation based, human-centric problem solving method embraced by industry leaders and corporations such as Apple and Google, but not yet embraced within the Air Force. The CyberWorx design thinking process is a transdisciplinary method that breaks down silos of standard organizational structures. Organizations naturally form structures based on specializations to facilitate deep expertise, but these structures often impede creativity, collaboration, and knowledge sharing vital to innovation. CyberWorx deliberately reaches across specialties to bring diverse perspectives to a problem in a non-threatening environment. This evokes ideas that would otherwise be missed or stifled. The transdisciplinary design approach teases out meaningful solutions that are intuitive and desirable to Airmen.

> The CyberWorx design thinking approach deliberately breaks through the military's hierarchical and mission silos to find hard-hitting answers.

Air Force CyberWorx offers facilitated design thinking sessions that bring stakeholders, industry and academic experts together to develop solutions to hard problems. These sessions are tailored to best meet Air Force needs with differing lengths based on time sensitivity and CyberWorx capacity. One method, which maximizes the educational benefit to cadets and industry partners, is to offer a design course where the semester long design project is a challenge being worked for AF stakeholders. The goal of such a design project is to develop low fidelity prototypes that clearly convey the desired Airman experience and the technical and policy developments needed to bring that experience to fruition. These projects help refine the requirement by seeking the right problem to solve and find meaningful solutions by exploring a wide range of possible answers to the design problem.

For the Air Force Cyber Command and Control (C2) Design Project, CyberWorx brought together 25 cadets from the United States Air Force Academy (USAFA) and industry partners to travel to locations across the Air Force for concentrated research visits with the Airmen who are conducting C2 in aspects of the cyber domain. For this report, it's important to understand something 2hat is not widely-known about the definition of the cyber domain: there is one! That

definition is taken from our Joint doctrine, Joint Publication 3-12, and reads as follows, “A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” That last phrase includes processors and controllers “embedded” into weapons systems, including aircraft and spacecraft. Many weapon systems were built and connected before cyberspace became a contested warfighting domain. The Air Force is learning how we will need to fight and preparing itself for leveraging operational advantages from and through cyber in digital-age wars.

The design team was to rethink how the Air Force does C2 for its cyber capabilities to improve the user experience of Airmen involved in the fight and day-to-day operations at all levels. The goal was to develop a concept for an improved structure, technologies or processes to present at the end of the semester to the Air Staff rewriting the Air Force Instructions guiding C2 of Cyber. Air Force CyberWorx projects do not aim to deliver a perfect solution to the tough operational problems taken on, but to deliver ways ahead to rapidly improve warfighting based upon the findings of the design teams.

Participants

The design course was attended by a diverse group of civilians from industry whose differing perspectives provided unique values that were distinct from the military members and government civilians interviewed. The CyberWorx design thinking approach deliberately breaks through the military’s hierarchical and mission silos to find hard-hitting answers. This design project included industry partners and cadets from USAFA with input from airmen and government civilians at the visited locations and guest visitors to the design studio in Colorado Springs. The design team reached out to individuals from five Air Force bases: Lackland AFB, Peterson AFB, Schriever AFB, Scott AFB and Langley AFB. A project officer at each location set up research interviews and visits for the design teams with organizations involved in C2 of cyber to observe (using ethnographic research methods) the Airmen in action.

Design Problem

Define and Refine C2 for Communications and (emerging) Cyber Squadrons: The current cyber environment requires constant innovation to combat cyber risks to Air Force networks and warfighting capabilities. The Air Force intends to strengthen active cyber defense and mission capabilities in this warfighting domain, which affects all other warfighting domains. Questions and concerns regarding the status of current operations were observed at all locations and considered by the design team, resulting in several immediate changes taking place at the bases as a result of the conversations. The subsequent consideration of "themes" were devised by the design team for the Air Force to consider as potential improvements in rewriting C2 policy and integrating advancing technology for the military service.


BND BELLEVILLE NEWS-DEMOCRAT

SCOTT AIR FORCE BASE NEWS FEBRUARY 9, 2017 12:44 PM

AF Academy 'Cyberworx Cadets' visit Scott AFB

Theme Discovery

The original design problem given by the Pentagon called for "refining and defining of C2 structure of cyber communication squadrons." Results of the field research, however, led the design team to broaden the areas of concern beyond just the organizational structure. These were refined during the project to three overarching topics or themes:

- ***Command and Control Structural Reframing***
- ***Patching***
- ***Decentralized Execution***

The design team's analyses of the users' work environments, to include current advantages, and current frustrations within the system (not just technology, but processes and organization) led to a revised problem statement. CyberWorx design groups conducted a series of interviews with cyber experts in both the private sector and department of defense. Insight from the interviews and site visits exposed a diverse range of experiences with Cyber C2 and provided a greater understanding of the problem at hand than would be available from looking from only one perspective (for example, from the Pentagon, or from the 24th Air Force, the AF's Cyber Component to the US Cyber Command).

Taking the three themes above into consideration, the design teams formulated potential solutions to help advance the Air Force along the thematic lines to combat current risks and extend operational advantages in its cyber operations. These proposed solutions were then prototyped and tested rapidly using least viable product (agile) methodologies to indicate where we would likely be successful and find good possibilities to make the biggest impact on warfighting once implemented.

Design Themes and Personas

Progressing through the design process required teams to analyze and organize information in a manner to communicate efficiently with stakeholders. This communication is aided by the development of personas--archetypal descriptions of user behavior patterns into representative profiles--to humanize the design focus and test proposed scenarios and prototypes. The three themes affect operations at all levels and are organized here to move from the Strategic to the Operational to the Tactical issues prevalent within the cyber warfighting domain.

At the squadron level, the persona of **Airman Leigh Stitzer** was created to represent how a cyber airman will interact with the system and changes at the lowest level. She is an enthusiastic airman who is great with computers, networks, gaming and technical ideas, but is not a people person. **SSgt Roger Cypher** is also an enlisted cyber expert who is dedicated to deterring and reducing cyber threats to Air Force operations on a mission defense team at the squadron. At the Wing level, **Maj Pat Summers** serves as a Non-Kinetic Effects Officer, representing a career cyber officer and an expert in that field and the application of cyber effects in all warfighting domains. For the purpose of representing upper leadership at the operational and strategic levels, **Colonel Jan Rogers** was created. She is an outspoken senior officer at the 24th AF who prides herself in being an agent of change. The base contracted cyber services support is represented by **Ms. Deborah Thompson**. She is a government contractor who has worked in cyber her entire life on the same base. Her experience outlasts four presidents; she has changed companies as different parent companies win the base-level contract (she has always been offered a position with the new winner) and her company “reports” to the contracting officer representative in the cyber squadron.

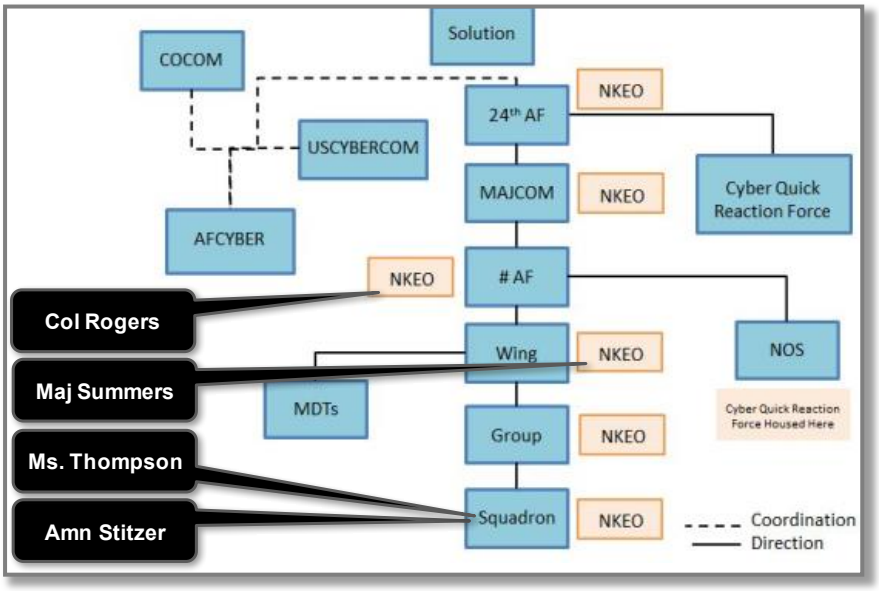
C2 Structural Reframing & Further Decentralized Execution

Airman Stitzer is an average cyber airman who loves what she does despite the less than favorable conditions of deteriorating facilities and under-funded IT infrastructure (some of the routers were installed at the base when she was still in middle school). Airman Stitzer is an introverted woman who knows the back of every computer and network topology on base, but she is not comfortable in social situations or dealing with people in general.

Airman Stitzer currently receives differing orders with varying levels of commands from different sources and then must make the decision of which order to complete first, or complete at all,

during her day. She receives orders from her line staff from the wing and base that fall under her ADCON, and directly influence her career progression; but she also receives orders from the MAJCOM Communications Focal Point (or MCCC) and 24th Air Force (wearing its "AFCYBER hat") on more operational endeavors, constituting OPCON for her unit, although that distinction is fuzzy for Airman Stitzer. The OPCON orders may have a higher priority for the Air Force, but if Airman Stitzer does not complete her ADCON orders first, her boss will be on her case and her career may suffer. The observed common solution for Airmen like Leigh Stitzer is to focus on the base issues that directly influence them and their careers, leaving the operational orders for a later time. Airman Stitzer and her leadership spend a lot of time frustrated about trouble tickets they don't have permissions to fix themselves that impact their wing's missions. Airman Stitzer feels sorry for her squadron commander who tries to keep morale high, despite the lack of base-level permissions and the high pressure to keep data flowing and IT systems patched to meet the never-ending steam of technical orders.

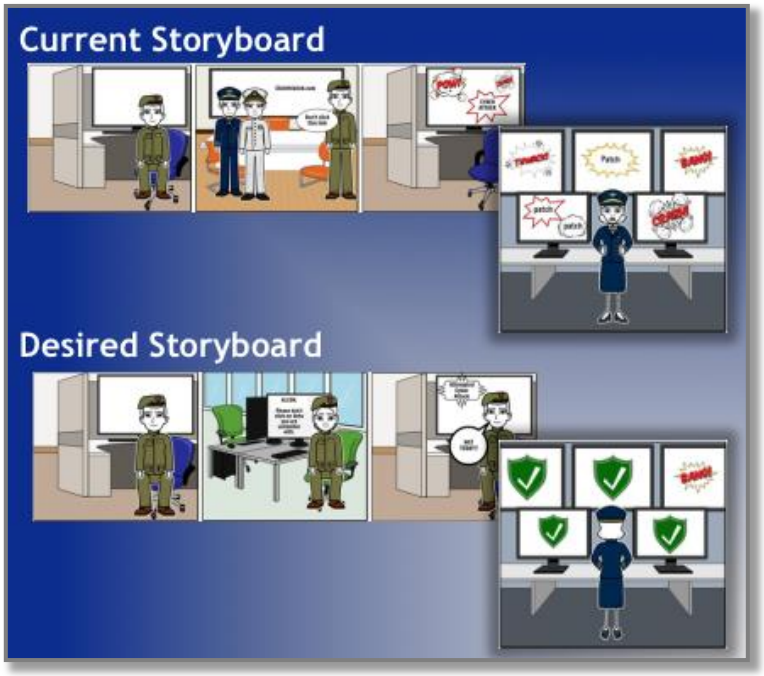
A reworked framework of the command would allow for airman in communication squadrons and cyber squadrons to have a single line of command so that OPCON and ADCON come from the same line, eliminating conflicts of interest to improve Airman Stitzer (and her supervisors') operations. For example, the removal of the MCCC would mean not only a simplified C2 structure, but would make valuable positions available to create a new position, which the design team is calling a Non-Kinetic Effects Officer (NKEO) or "the Orange Billets."



Major Summers is one of these NKEOs who will be found at every level of the C2 chain from squadrons up to the Numbered Air Forces and Major Commands to help the transition between communications and cyber squadrons. Major Summers is a career cyber officer who considers herself an expert, but has never had the opportunity to attend cyber-focused events like DEFCON, either on her own or as part of her training. She was extremely frustrated with the old reporting lines and the roundabout way that orders would finally reach the operators at the base. Her new job as NKEO will allow her to absorb the "translation duties" of the MCCC and communicate with either the new Mission Defense Teams and contracted enterprise service providers or the communications squadrons that have yet to transition to cyber squadrons. She will serve as the cyber expert and be the expediter of the reporting lines between Joint and Air Force, upper/strategic echelons and bases. She is expected to keep up with industry and joint trends and to work with squadrons

and wings on managing cyber talent and implementing ideas from Airmen across the service to shorten decision-cycles and make the Air Force more lethal.

Another NKEO, Colonel Rogers, sits at the Numbered Air Force (NAF), and will communicate with the Network Ops Centers for larger strategic issues within cyber and will be in the reporting line for Major Summers. Major Summers will communicate with Colonel Rogers, an outspoken senior officer who does not necessarily have direct experience in cyber, but is well-versed in the strategy and warfighting operations of the NAF(s) in her command. Colonel Rogers takes orders from the NKEO at AFCYBER, and while she may not have the technical expertise of the career cyber officers, will relay the orders and help work priorities for units to the best of her abilities while motivating those below her. Major Summers will be able to take these orders and put them into the technical words needed for the airmen at the lower ends of the chain while also communicating strategic intent to the MAJCOM and NAFs and Wing NKEOs, ensuring more streamlined lines of communication between cyber experts and non-cyber commanders at all levels. Airman Stitzer will now receive the precise communications and cyber orders using the network permissions she needs from a single source, allowing her to complete these orders in a timely manner and without the massive conflicts of interest that we found is the current norm at locations.



Cyber Quick Reaction Force (Cyber QRF)

Due to the permanent threat of cyber attacks, and the instant nature of the cyber domain, a Cyber Quick Reaction Force (CQRF) will remain at the top of the C2, owned day-to-day by the AFCYBER and positioned (at the Network Ops Center or elsewhere) in order to address immediate and pertinent issues. They are the team that can switch hats on a moment's notice, based on the duty at hand, to immediately address the threat and other issues. This team is the immediate, elite cyber force that will handle issues that cannot afford the time it takes to go through the typical chain of command to be addressed. This force will be modeled on the Special Operations quick reaction forces. This force will be broken down into several teams that will rotate through operational readiness statuses, Red, Amber, and Green, in order to remain refreshed and trained. Red status indicates that that team is training and exercising, Amber indicates that the team is validating and preparing for the operational duties, and Green indicates that the team is ready to go and always on call for any problems that may arise. Much like the Special Operations Forces, this force is focused solely on the jobs at hand.

Non-Kinetic Effects Officer (NKEO)

The purpose of the “Orange Billets” is to help the cyber career field reorient or transform from a services-oriented communications career field at multiple levels to a defensive- and offensive-cyber and mission-assurance-oriented career field. These positions start with the Subject Matter Experts at the squadron level and will help ensure and indicate the needed training for these billets, filled by O-2s and E-4/E-5s and higher (at higher echelons), who also help the service transition to the multi-domain warfight with integrated effects for our digital age.

To streamline network defense and facilitate faster response times than are currently the norm at the observed units, network defense operations and permissions would be pushed down to the lowest level possible. At the squadron level, there will be a **Mr. Brothers** who could represent both SSgt Cypher, trained to be a 1B471 (Cyber Warfare Operations Craftsman) or a civilian equivalent such as Ms. Thompson who is contracted to provide active security. In either case, the service would be the same: the frontline defense crucial for rapid detection and mitigation of threats to Air Force missions. The Mission Defense Teams (MDTs) will act as the expert teams when the threat grows beyond the capabilities of a single actor. The default will be to address the threat immediately instead of automatically relaying it to the CQRF for action. This immediate response will keep systems operating on the network for as long as possible, allowing Airmen across the base to fight through and do their missions, even while the cyber risk and findings are being reported for enterprise-wide responses and mission assurance.

Mr. Brothers may be attached to a specific squadron and have access to all systems under that squadron’s purview. Mr. Brothers will monitor the systems on the network at all times. Additionally, anti-malware software and other automated threat-intelligence systems and ecosystems will alert Mr. Brothers when there is a threat on the network so he can notify those whose missions may be impacted by the threat and isolate the system to prevent further infiltration. He will attempt to defeat and neutralize the threat, effectively shortening the time that systems may be offline and helping to coordinate unified responses to prevent impacts on other like units across the enterprise.

To mitigate confusion and establish transparency with the 24th Air Force, Mr. Brothers will be responsible for reporting to the NKEO (Maj Summer) to keep the 24th Air Force and other NKEOs along the chain informed as to what is being implemented and other units with similar mission systems that may be vulnerable. However, Mr. Brothers will not have to report directly to the 24th to prevent the possibility of having a dual chain of command. This will help the wing commanders assure their missions in the face of determined enemy attacks or other cyber hazards that must be fought through.

Patching & Decentralized Execution

With any operating system or network configuration, adversaries identify and exploit vulnerabilities much like viruses swarm a small cut in the skin. The patching process seeks to

find the cuts in the Air Force using “patches” that fortify and cover the network and weapon systems vulnerability to prevent intrusions and ensure security in all Air Force operations. The deliberateness in which the Air Force administers these patches determines whether warfighters have communications on the battlefield and coordinated effects from all domains. It can determine whether foreign foes will have access to highly classified data and, with an ever-advancing reliance on information dominance, may ultimately determine victory or defeat.

One of our industry partners, Kris Kistler, Chief Information Security Officer at Centura Health stated that “The magic number is eight.” From the point a company releases a patch to an information system to be applied, it will take at the most eight days for an adversary to reverse engineer the patch and be ready to exploit the underlying vulnerability. Our interviewees, including those from the NOS, stated that our current process takes quite a bit longer than this magic number of days that is well-known by industry (and adversaries).

This section outlines a solution to the glaring problem by first describing the Air Force’s current state in terms of how our interviewees believed patches are tested, how they are applied through the operational chain of command, and how individual bases communicate to solve configuration issues.

We will propose a solution by first setting the vision for the ideal patching process and then prescribing steps the Air Force can do to get there. Ultimately we propose the following three-pronged approach: (1) establish a virtual environment that mimics the Air Force network to quickly test patches with no risk; (2) create a configuration management tool that tracks the status of cyber assets; and (3) open up an official line forum as a collaborative space for individual bases to address their issues rapidly as patches are applied.

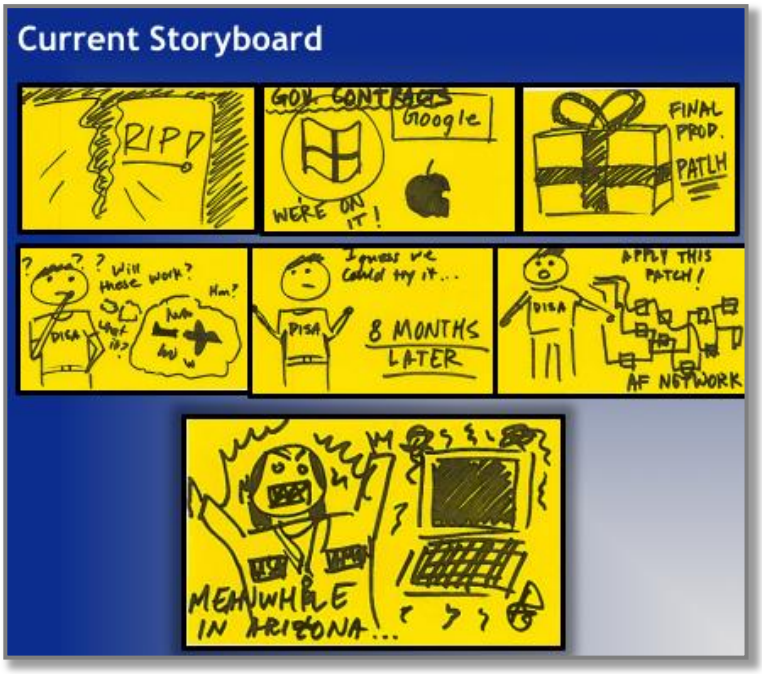
Current State

The design team for this project visited Scott, Peterson, Schriever, Lackland and Langley Air Force Bases and conducted interviews with commercial CyberWorx partners and companies such as Google and Route 9B. Upon the arrival at the bases we toured facilities and interviewed enlisted Airmen and Officers alike to get a firm understanding of how cyber

operations were conducted at all levels of operation. In our interviews, some of our biggest takeaways w the issues regarding timeliness of patch implementation. With hackers being able to reverse engineer patches in under 8 days, we need to expedite patching to mitigate the warfighting vulnerabilities that come about through slow patching to prevent enemies from attacking at the time of their own choosing.

Most of the slow timeline stems from a systemic issue of how testing of patches is done at multiple levels without effective communication between our bases, and moving back up and across the chain that are telling them to apply the patch.

When a patch is created by the vendor, it is then passed to DISA. Upon arrival, DISA performs an initial review to see if the patch is legitimate and then pass it to USCYBERCOM, which initiates testing with some baseline system configurations and then passes it down to the different services, including the 24th Air Force. The 24th Air Force then takes the patch and does a test based on the Air Force Standard Image to see if it can be implemented by the NOS and individual bases. If they see that the patch can be implemented, it is passed down and added to an implementation timeline for the bases to complete by a certain date.



While a significant amount of stovepiping occurs in the current process, some communication does actually happen between offices which are associated with units at both the bases and higher echelons; however, every issue has to raise up to that level before it is addressed. There was not a standard way for SSgt Cypher to get his findings and concerns addressed. These communication issues are partially addressed through tools such as MilSuite; however, Airman Stitzer also turns to technology like social media—for example, an unsecured Facebook page—outside of the official network to work through patches and troubleshooting. SSgt Cypher uses the same tools to communicate with the other bases. They prefer closed group Facebook over other communication tools because it is familiar and easy to use—their everyday use (on their own machines and government systems) means they can stay well-connected to friends and colleagues while still doing needed work.

The MCCC attempts to facilitate these discussions of patches (in official channels), but other than aggregating insights from the base and slowly passing them forward, the MCCCs have no real insights and, instead, are acting as middlemen in the communication process. As such,

they could play a role trying to connect disparate systems, but are literally copy-pasting to try to ensure that information on outages and impacts of patches are properly communicated, even if context is not captured.

A lack of knowledge of the current configurations and the settings that are implemented add to the overall confusion that makes testing and patching so difficult. A lack of genuinely effective tools for configuration management means that there are many different configurations and mission programs which are installed on computers that do not work well together. Those configurations are not well known, even by Airman Stitzer and SSgt Cypher, who have always been kapt at arms length from mission systems and have few permissions to make firewall fixes, often broken by pushed "updates" and uncoordinated configuration changes affecting their base.

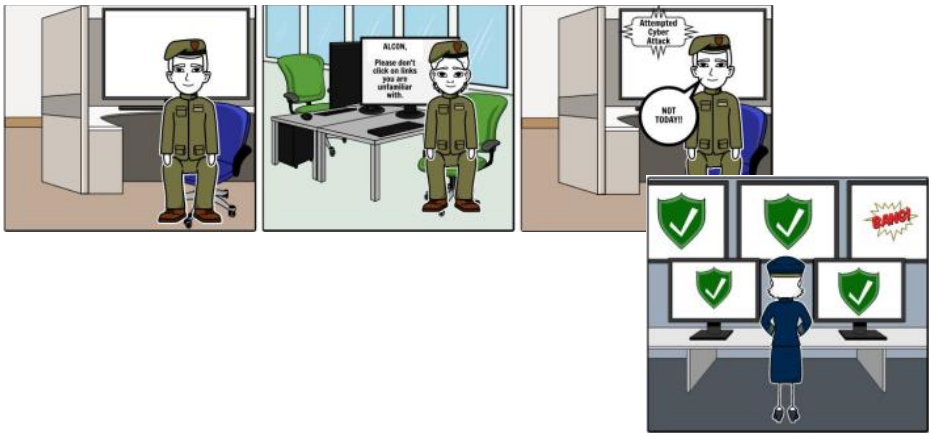
Even though there is a requirement that 10% of a network is labeled for "testing" and this is supposed to represent a full sliver of the network, the "testing" portion is often comprised of active computers, causing mission impacts on certain subsets of users, and is often ignored due to the mission needs at bases and lack of "extra" assets. Additionally unique software and systems, such as those in the Air Operation Centers, are not included in the testing set, further limiting the picture of the tested configurations and excluding some of the most critical mission systems from receiving patches that would enhance resiliency.

Despite the efforts by DISA and other organizations to help reduce the risk of applying patches, according to those we observed, the only way to really know what's going to happen when a patch is applied is to try it, leading to a lot of frustration by Amn Stitzer, SSgt Cypher, Ms. Thompson and their wing commanders whose missions are unexpectedly degraded or stopped.

An Improved State

Keeping the aforementioned concerns in mind, we will now address what an improved state of this patch process could look like if it were functioning as efficiently as possible. The three main issues to see improvement on—common themes throughout our interviews as well at our base visits—were the centralization of a virtualized network, which does not now exist, the sharing of info across individuals working on portions of AFNET, and configuration management.

As it currently stands, AFNET does not host a centralized virtual network where patches can be run and tested to understand the impact on mission-critical systems. Ideally, a centralized host (maybe hosted by DISA or the Cyber Proving Ground or AFNIC) with a variety of testing environments for all different types of patches would be available for rapid assessments. This will eliminate the need for the policy which states that 10% of computers on each base must be designated for testing, even though they are still functional user computers on the network. Using this centralized host, experts like SSgt Cypher from bases around the world would be able to access and test patches for mission systems on the same virtualized network, minimizing wasted time, repeated work at multiple bases, and allowing distribution of patch-testing workload to the base-level experts.



This implementation of a centralized virtual network also supports sharing of information concept as well, alleviating Amn Stitzer's inability to communicate with others facing patching issues. As discussed, we found a profound lack of communication at all levels throughout the patching process. Although formal means of communication to facilitate the sharing of information do exist, we found they are not widely used. Ideally, through the implementation of policy and providing user-friendly ways to carry it out, the Air Force will move to use of a collaborative network forum, like an improved MilSuite. This will ultimately increase the sharing of information among cyber squadrons throughout the Air Force and facilitate faster patching solutions, reducing the risk of vulnerabilities in the system.

We also found configuration management to be a prevalent issue within the framework of the patching system. Right now, there is no centralized configuration management system on AFNET that is reliable and used routinely. This means that, while there are thousands of systems on the network, there is no centralized system to de-conflict settings, manage security requirements, and similar important steps. Increasing the awareness of the systems on the network (toward AFIN from AFNET) and how they all work together through the implementation of a centralized configuration management system will lead to improved, faster patching.

With the centralized virtualized environment, leaders like Col Rogers and Maj Summers will be able to refer to the virtualized machines (or digital twins of real systems) for their specific bases to see what their system configuration entails and how it is performing compared to other systems on the network or on other networks accomplishing similar missions. This centralized virtualization of AFIN will host the gold standard for the base specific networks and allow the

use of centralized tools and intelligent algorithms to help identify vulnerabilities and problems for systemic improvement of mission assurance.

The benefit of a centralized environment could also extend to improving enterprise-level patch management as patches could also be categorized by urgency and risks managed and communicated more easily than is currently done. The only way that a base is aware of the status of similar patches at other bases is through the limited use of milSuite (or social media); otherwise there is a significant lack of knowledge of the status of the patch implementation by Amn Stitzer and no effective way for a NKEO at any level to understand and predict mission impacts or risks.

Summary of Benefits

The proposals presented in this report address several underlying issues the Air Force faces in developing a cyber workforce and further operationalizing the cyber domain. These issues were raised by participants in the design process and by key stakeholders we interviewed. It is important to note many of these recommendations are extensible to other specialties (outside of cyber) and may represent a desired solution for much of our workforce: How, for example, are personnelists communicating about and modeling policy impacts on the future workforce and changes to the systems used to manage Airmen's assignments?

The modernized framework is helpful to reduce dissatisfaction of Airmen in the cyber workforce and help the transition to the cyber squadron and the multi-domain future of our Air Force. The ability to accurately assess the capabilities of communications and cyber expertise is necessary. A redesigned cyber framework that focuses on a streamlined and decentralized C2 structure will help overcome the current mixed signals for SSgt Cypher and other base-level Airmen. The creation of Mission Defense Teams will allow teams to tackle the unique cyber problems specific to each base's mission. These teams may be tasked out to various units as necessary - specifically with the goal of cyber defense in mind. The creation of NKEOs within the C2 framework will maintain the technical expertise of the cyber and communications mission sets throughout the entire chain of command while better communicating outside of cyber specialists. Their expertise will help accurately task strategic, operational and tactical issues at all levels, unlike the current system in which multiple chains of command task down to a single overwhelmed unit with no clear sight picture or permissions to make AF warfighting better.

Cyber capabilities are crucial to the success of the Air Force. Rapid response to threats, specifically at the base level, will allow for a quicker turnaround time to reinstate secure connections and protect vital systems that may have been isolated during the neutralization of the threat. Instead of sending all threats to a centralized point for defending the network, a person on the base will have the skills and a better perspective as to what may happen if various systems are taken off the network due to a rising cyber threat. This shorter turnaround time benefits those who rely on the isolated systems, allowing them to continue their work faster, promoting a more ready and effective Air Force. Problems beyond the skills at base level will be routed to a Cyber Quick Reaction Force, who will seek quick and efficient solutions to pertinent strategic issues and base specific problems.

Where to Start Small for Big Impacts

Based upon the research this semester, the CyberWorx design team recommends a phased approach toward implementing all aspects of this proposal as described below.

Decentralize Control & Establish Cyber QRF

1. Implement Mission Defense Teams at each wing for base cyber defense.
2. Establish a Cyber QRF to allow for proactive engagement and an immediate retort to pertinent threats in cyber affecting AF missions. Augment this team with data analytics and threat response tools (moving toward AI-augmented teams).
3. Streamline the C2 framework for standardization and ease of command.
4. Eliminate or re-purpose the MCCC as currently they are only a middleman, reporting mechanism whose function could be absorbed by the normal chain of command.
5. Implement NKEOs to fill the role of solving cyber and communications issues as the field matures.

Improve Cyber Expertise at Bases (with NKEO)

1. Train an Airman as a 1B471 or hire a civilian equivalent/contractor to provide on-site technical expertise for an NKEO.
2. Attach them to all communications squadrons to prepare and blend cyber and comms during the transition of the career fields.
3. Allow immediate remote access of each system to the network defender.
4. Assign them to a NKEO who will coordinate with the 24th Air Force.

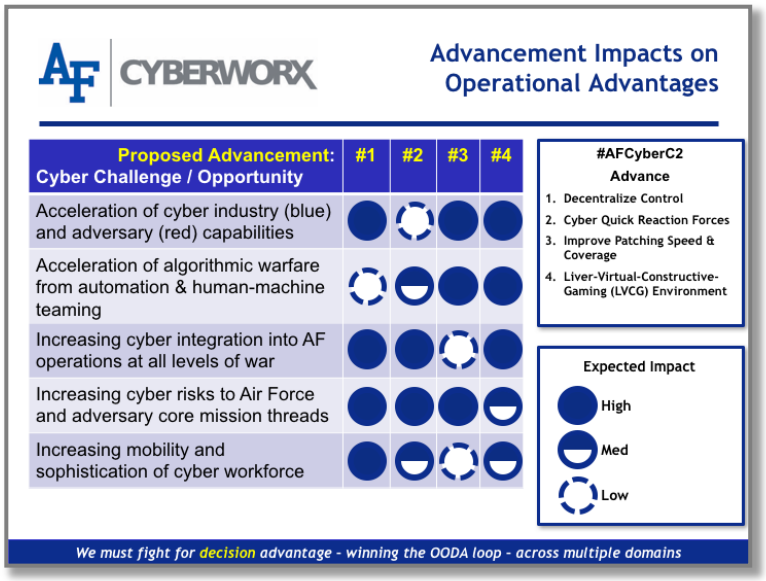
Improve Patching Speeds & Coverage

1. Virtualize the testing environment, hosted at the 24th AF or other entity at the enterprise level. Make the same environment available for gaming and development.
2. Have a virtualized instance of every type of configuration that individual bases have in order to speed up testing and allow for better configuration management

3. Communicate at all levels about issues and solutions that bases have with correcting and implementing patches.

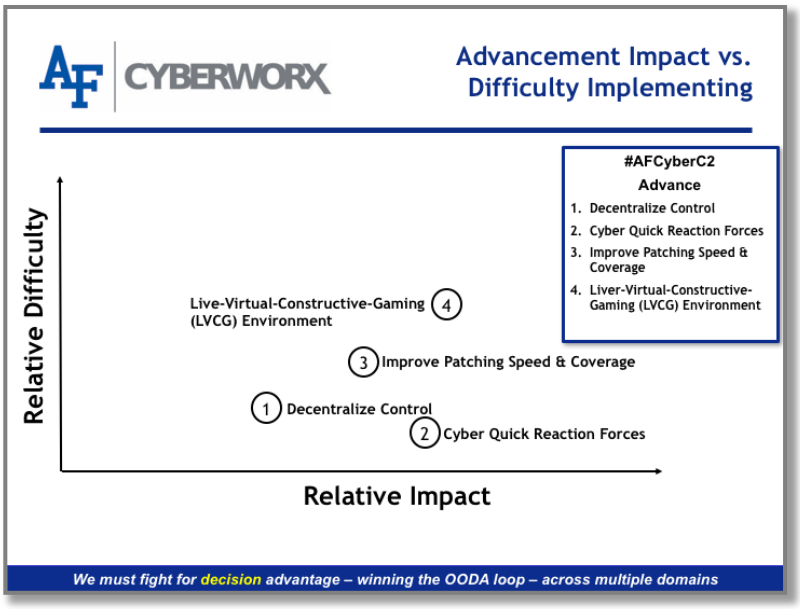
Summary: Ops Advantages + Fast Track

The CyberWorx "three slide summary" section is designed to help you consider the recommendations in this report by weighing the operational improvements proposed against the current cyber challenges and opportunities we face as an Air Force.



In deciding what to do, the decision to do nothing is a decision and brings its own risks. Thus, the "fast track" slide spells out an easy set of actions to take at minimum to start trying to improve and to put the Air Force on a path of discovery in overcoming the challenges that drove this design project.

We recognize we live in a resource-constrained world. Each advance proposed in this report is graphed below: The graph compares the advance's relative impact on the ability of the Air Force to maintain information and decision dominance (x-axis) against the difficulty (e.g., expenditure of time/treasure, cultural evolution, policy change) needed to implement that advance (y-axis). Cultural changes, like some of those proposed in this report, are not easy, but they are possible and needed for success in our digital, cyber-contested world.



CYBERWORX ™